UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/724,873	11/28/2000	Raymond C. Pang	X-805-7 US	8398

24309 7590 02/16/2005

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/724,873	PANG ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) *9-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *9-25* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/21/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated September 21, 2004 with the amendment of claims 1-8 and the addition of claims 9-25.

2. Claims 1-25 are pending.

Response to Arguments

3. Applicant's arguments filed September 21, 2004 have been fully considered but they are not persuasive.

4. The applicant argues that the combination of the system of Galovich and Kim does not show a PLD having an encryption key in which a plurality of key bits define an encryption algorithm and at least one bit for indicating whether more keys will follow. The examiner maintains that in apparatus (Fig. 1, element 10), the encryption circuit comprises a PLD (col. 7, lines 6-19), and the PLD is configured to perform some or all of the encryption wherein the encryption circuit may perform many encryption techniques such as DES, a block cipher with 64 bit block size and uses 56 bit keys (col. 7, lines 59-67). Galovich does disclose a PLD having an encryption key in which a plurality of key bits define an encryption algorithm.

5. The applicant stated on page 7 "Kim does not implicitly disclose indicator bits to indicate whether more keys will follow". This language is not in the claim.
As to claim 1, "at least one bit for indicating whether more keys will follow", this claim language is broader than the "indicator bits to indicate whether more keys will follow".

Furthermore, on page 7 of the response, the applicant argued that Kim uses a counter to determine whether application of any additional keys is required as supposed to indicator bits. A counter output is composed of bits. Therefore the counter output is at least one bit indicating whether more keys will follow.

6. The applicant argued that the motivation for combining Kim with Galovich is improper. The examiner maintains that Galovich discloses several encryption techniques, including DES (col. 7, lines 59-67). Kim also discloses DES technique and further states "the secret key is not uniformly assigned to all of the 64 bit blocks" (col. 1, line23), therefore Kim discloses a system to uniformly assign key values so as to increase the strength of ciphertext data.

Election/Restrictions

7. Newly submitted claims 9-25 directed to an invention that is independent or distinct from the invention originally claimed for the following reasons:

a) Claims 1-8, drawn to a programmable logic device, classified in class 713, subclass 189.

b) Claims 9-25, drawn to method for configuring a programmable logic device, classified in class 713, subclass 189.

The inventions are distinct, each from the other because of the following reasons:

8. Inventions a and b are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, the PLDs of invention a can be

configured with other method than that of group b and invention b can configure other PLDs than that of group a. See MPEP § 806.05(d).

9. Because these inventions are distinct for the reasons given above and the search required for Group b (713/189; 713/193; 380/277), i.e. searching for storing plurality of decryption keys and storing configuration data in configuration memory of the PLD, is not required for Group a (713/189; 326/39), restriction for examination purposes as indicated is proper.

10. Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 9-25 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over the admitted prior art in view of Galovich, US 6,560,709 in view of Kim, US 6,246,768.

a) **As to claims 1-2 and 5-8**, the admitted prior art discloses a programmable logic device (Fig. 1, element 10) comprising a plurality of programmable logic resources (Fig. 1); a configuration control circuit coupled to the plurality of programmable logic resources (Fig. 1, element 14); a key memory coupled to the configuration control circuit (Fig. 1, element 12).

The admitted prior art does not disclose a programmable logic device having stored therein a plurality of key bits for defining an encryption algorithm and at least one bit for indicating whether more keys will follow.

Galovich discloses an apparatus and method for the secure transmission of credit card data over an Internet connection comprising an encryption circuit encrypts the scanned card data from card reader (Fig. 1, element 14; col. 7 lines 10-11) which reads on an encryption key stored in a PLD comprising a plurality of key bits (col. 7, lines 59-67) for defining an encryption algorithm.

Galovich fails to disclose at least one bit for indicating whether more keys will follow.

Kim discloses a data encryption system (Fig. 1, element 100) for encrypting input plaintext data comprising a key scheduling device (Fig. 1, element 300). At the key scheduling device, 16 sets of round subkeys are used in encrypting the input plaintext data in each of 16 rounds, are derived by using the preset master key K (col. 2, lines 48-52). It implicitly discloses some indicator bits in the master key indicate whether more keys will follow, whether key is a first key which corresponds to first round, middle, last key which corresponds to the 16^{th} round or only of a set of keys (claims 2 and 5-8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of bit indicating whether more keys will follow, as Kim teaches, in the system of Galovich so as to uniformly assign key values in order to increase the strength of ciphertext data (col. 1, lines 23-27).

b) **As to claims 3-4**, Galovich discloses the encryption key wherein the plurality of key bits comprises 56 bits and wherein the encryption algorithm comprises the DES algorithm (col. 7, lines 59-67).

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
2/14/05

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER